REMARKS

The present Amendment amends claims 1-10, 12 and 13 and cancels claim 11. Therefore, the present application has pending claims 1-10, 12 and 13.

Claims 1, 2, 5-10 and 12 stand rejected under 35 USC §103(a) as being unpatentable over Rubert (U.S. Patent No. 6,366,915) in view of Ho (U.S. Patent No. 6,148,342); and claims 3, 4, 11 and 13 stand rejected under 35 USC §103(a) as being unpatentable over Ho and further in view of Ote (U.S. Patent No. 6,023,506). This rejection is traversed for the following reasons.

As indicated above, claim 11 was canceled. Therefore, the 35 USC §103(a) rejection of claim 11 as being unpatentable over Ho in view of Ote is rendered moot. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

With respect to the remaining claims 1-10, 12 and 13, the above described rejections are traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 1-10, 12 and 13 are not taught or suggested by Rubert, Ho or Ote whether taken individually or in combination with each other as suggested by the Examiner. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw these rejections.

Amendments were made to each of independent claims 1, 10 and 12 so as to more clearly recite that the present invention is directed to a data relay server for accessing a database server via a communication network in accordance with a query for a database received from a client computer, the database server itself and

a database access method which corresponds to the functions performed by the database server.

According to the present invention the data relay server includes first means for encrypting retrieval condition data included in a query received from a client computer, second means for producing a query message destined for the database server including the retrieval condition data encrypted by the first means and an identifier of an encryption function used to generate the encrypted retrieval condition data, third means for transmitting the query message produced by the second means to the communication network, fourth means for receiving from the database server via the communication network, as a retrieval result, data matched with the encrypted retrieval condition data retrieved by matching the data with the encrypted retrieval condition data, wherein the matching is performed by encrypting at least one data item read out from the database in the database server using an encryption function designated by the identifier in the query message and comparing the at least one data item to the encrypted retrieval condition data, and fifth means for producing a response message for the client computer based on the retrieval result received by the fourth means and transferring the response message to the client computer.

The database server include a database in which service information is stored and a database management system for searching the database for service information matched with a retrieval condition designated by the query message.

According to the present invention the database management system includes means for encrypting a specific data item designated by the retrieval

condition and read out from the database when the query message includes encrypted retrieval condition data and an identifier of an encryption program used to generate the encrypted retrieval condition data and retrieving service information matched with the retrieval condition by matching the encrypted specific data item to the encrypted retrieval condition data, wherein the specific data item is encrypted using the encrypted program identified by the identifier, and means for transmitting a response message including the retrieved service information to the source of the query message.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record whether taken individually or in combination with each other. Particularly, the above described features of the present invention are not taught or suggested by Rubert, Ho or Ote whether taken individually or in combination with each other as suggested by the Examiner.

Rubert teaches a method and system for efficiently retrieving information from one of several databases. As taught by Rubert, the system therein acts as an intermediary between users and databases so as to manage user access to the databases so that query specification, query execution and query result retrieval can occur efficiently and securely. However, as recognized by the Examiner in paragraph 4 of the Office Action Rubert does not teach or suggest the encrypting of retrieval condition data included in the query received from the client and submitting a query message to a database server including the encrypted retrieval condition data so as to retrieve matching data as in the present invention.

The Examiner recognizing the above described deficiency of Ruberts attempts to supply such deficiency by combining Rubert with Ho. The Examiner alleges that Ho teaches the encryption of retrieval condition data. Upon review of Ho, it is noted that a source terminal 104 as illustrated in Fig. 1 thereof produces a data packet 116 which includes an encrypted data access request 124 and an encrypted identifier 112. As described in col. 3, line 14 through col. 4, line 50 of Ho, the encrypted identifier 112 is encrypted using a first encryption code and the data access request 124 is encrypted using a second encryption code. Further, as taught by Ho, the data packet 116 is transmitted to an identifier database 128 having the codes necessary to decrypt identifier 112. As per Ho, the identifier database 128 converts the data packet 116 into a data packet 148 after performing user authentication. In this case according to Ho, because the identifier database 128 does not have the decryption key needed to read information contained in the database access request 124, the data access request information remains protected from the system administrator of the identifier database 128. Thereafter, Ho teaches that the data packet 148 as generated by the identifier database 128 is transmitted to a data request database 152 having the program and the code necessary to decrypt the subject data 144 and the data access request 124 in the received data packet 148 so as to perform data access request based on the data access 124.

It is quite clear from the above that both Rubert and Ho fails to teach or suggest the unique features of the present invention as now more clearly recited in the claims. As per the above, the present invention provides a completely secure

system in that the retrieval condition data remains encrypted and data to be retrieved from the database that may match the encrypted retrieval condition data is itself encrypted using a function that encrypted the retrieval condition data. As clearly recited in the claims, the query message sent from data relay server to the database server includes the encrypted retrieval condition data and an identifier of an encryption program used to generate the encrypted retrieval condition data. This feature of the present invention allows for security in the query message being sent from the relay server to the database server. Further, according to the present invention the database server encrypts at least one data item read out from the database with an encryption program identified by the identifier and then attempts to match the encrypted data item with the encrypted retrieval condition data. If a match results then the data item is used as the retrieval result being sent back to the data relay server for eventual transmission to the client computer. Such features are clearly not taught or suggested by Rubert or Ho.

Thus, both Rubert and Ho fail to teach or suggest second means for producing a query message destined for the database server including the retrieval condition data encrypted by the first means and an identifier of an encryption function used to generate the encrypted retrieval condition data as recited in the claims.

Further, both Rubert and Ho fail to teach or suggest fourth means for receiving from the database server via the communication network, as a retrieval result, data matched with the encrypted retrieval condition data retrieved by the

matching the data with the encrypted with the retrieval condition data as recited in the claims.

Still further, both Rubert and Ho fail to teach or suggest that the matching is performed by encrypting at least one data item read out from a database in the database server using an encryption designated by the identifier of the query message and comparing the encrypted at least one data item to the encrypted retrieval condition data and producing a response message for the client computer based on the retrieval result received by the fourth means and transferring the response message to the client computer as recited in the claims.

Therefore, as is quite clear from the above, both Rubert and Ho suffer from the same deficiencies relative to the features of the present invention as now more clearly recited in the claims, and as such when combined fail to teach or suggest the features of the present invention as now more clearly recited in the claims. Accordingly, reconsideration and withdrawal of the 35 USC §103(a) rejection of claims 1, 2, 5-10 and 12 as being unpatentable over Rubert in view of Ho is respectfully requested.

The above noted deficiencies of both Rubert and Ho are not supplied by any of the other references of record namely Ote. Ote is merely relied upon by the Examiner for an alleged teaching that the query message includes an encryption program. However, at no point is there any teaching or suggestion in Ote of the above described features of the present invention shown not to be taught or suggested by Rubert and Ho. Accordingly, combining the teachings of Rubert or Ho with Ote still fails to teach or suggest the features of the present invention as now

more clearly recited in the claims. Accordingly, reconsideration and withdrawal of the 35 USC §103(a) rejection of claims 3, 4 and 13 as being unpatentable over Ho in view of Ote is respectfully requested.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references utilized in the rejection of claims 1-13.

In view of the foregoing amendments and remarks, applicants submit that claims 1-10, 12 and 13 are in condition for allowance. Accordingly, early allowance of claims 1-10, 12 and 13 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (520.40523X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120